UAR NUMBER: 400.02

TITLE: Wireless Network Policy and Procedure

ORIGINATOR(S):

Assistant Vice President of Technology

INITIAL ADOPTION: 11/06/2003

REVISION DATE(S): 07/09/2018

AUDIENCE: (SELECT ALL THAT APPLY)

✓ FACULTY ✓ STAFF ✓ STUDENTS ✓ VENDORS ✓ OTHER (SPECIFY): Visitors

PURPOSE:

Set forth the policy for using wireless data technologies and assigns responsibilities for the deployment of wireless services and the administration of the wireless data radio spectrum at Morehead State University (MSU). The document describes how wireless technologies are to be deployed, administered and supported at MSU.

SCOPE:

This policy applies to all Morehead State University (MSU) faculty, staff, students, visitors, and contractors. The policy applies to these persons participating in or supporting any activity in any academic and operational buildings, residence halls, and offices at all University locations, owned and leased.

DESCRIPTION (INCLUDE DEFINITIONS):

This policy governs the installation, operation, and maintenance of all wireless network devices utilizing MSU Internet Protocol (IP) network space, including private IP space within University networks, and all users of such devices, and governs all wireless connections to the campus network, frequency allocation, network assignment, and registration. It also applies to services provided over wireless connections to the campus network for colleges, departments, or divisions of the University.

The University provides and maintains computing and telecommunications resources to support the teaching, research, and administration activities of its faculty, staff, and students. A secure and reliable data network is a critical component of the University's infrastructure. While wireless networking devices can be useful tools for enhancing productivity and convenience, they can also negatively impact the availability and security of the University network if improperly connected or administered.

DEFINITIONS:
Wireless Network: local area network technology other than wired technology, including, but not limited to, technology that uses radio frequency spectrum, to connect computing devices to college, department, and division wired networks.

Access Point: electronic hardware that serves as a common connection point for devices in a wireless network.

Wireless Infrastructure: wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

Interference: the degradation of a wireless communication signal from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.

Point of Contact (POC): the person designated as having primary responsibility for a given wireless access point or network.

Virtual Private Network (VPN): the use of encryption to provide a secure means of connection over an otherwise unsecure network.

RESPONSIBILITY:
Wireless equipment and users must follow all acceptable use provisions stated in PG-55 "Technology Resource Acceptable Use" in addition to the more specific requirements described in this document. Wireless access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks. Responsibility for electronic communication resources at Morehead State University resides with the Office of Information Technology.

Deployment by Students
Students are not permitted to connect wireless access points to the campus network unless they are working under the direction of the Office of Information Technology. Wireless access points may not be connected to the student residential network.

Public Access Points
Responsibility for deploying wireless access points that are intended for use by the general University community resides with the Office of Information Technology.

Network Reliability and Interference

APPROVED BY:

VICE PRESIDENT: Chris Howes DATE: 7-9-18

APPROPRIATE INSTITUTIONAL REVIEW: _____ DATE: _____

PRESIDENT: Jay M. Morgan DATE: 7-9-18

400.02 Continuation pages

Network Reliability and Interference

In a wireless environment, network reliability is a function both of the level of user congestion (traffic loads) and service availability (interference and coverage). In an effort to provide an acceptable level of reliability, this policy establishes a method for resolving conflicts that may arise from the use of the wireless spectrum.

Wireless networking technology uses unlicensed frequency bands to create small local area network cells. Since unrelated devices such as cordless telephones, wireless audio speakers, and even microwave ovens may also use these same frequency bands, the potential for disruption of service exists when multiple devices are placed in close proximity to one another.

While OIT does not actively monitor use of the frequency spectrum for potential interfering devices, it responds to reports of specific devices that are suspected of causing interference and disruption of the campus network. Where interference between the campus network and other devices cannot be resolved, OIT reserves the right to restrict the use of all wireless devices in University-owned buildings and all outdoor spaces.

Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited. In the event that a wireless device interferes with other equipment, OIT will work with the affected departments to resolve the interference.

The Office of Information Technology is responsible for:

- Creating, maintaining and updating wireless plans, wireless policy and wireless security standards
- Maintaining a registration of all wireless access points on campus
- Resolving wireless communication interference problems
- Managing and deploying wireless communications systems
- Approving wireless communication hardware, software and installation services used by University schools/departments
- Informing wireless users of security and privacy policies and procedures related to the use of wireless communications in common areas
- Providing assistance to the campus community for the development, management and deployment of wireless networks
- Monitoring performance and security of all wireless networks and maintaining network statistics as required for preventing unauthorized access to the campus network

- Monitoring the development of wireless network technologies, evaluating wireless network technology enhancements and, as appropriate, incorporating new wireless network technologies within the University network infrastructure

The campus community, including Colleges, divisions and/or departments are responsible for:

- Adhering to Wireless Network Policy
- Informing wireless users of security and privacy policies and procedures related to the use of wireless communications

Security Awareness: Instructional materials will be made available to all wireless users via the University web site. The instructional material will include, but not be limited to the following topics:

- Authentication for wireless network access and protection of passwords
- Authorized use of wireless network technology
- Wireless interference issues
- Procedures for reporting wireless network service problems
- Procedures for responding to a suspected privacy or security violation
- Procedures for revoking user accounts due to termination of an affiliation with the University

Monitoring and Reporting: The use of wireless network technology is to be monitored by the OIT on a regular basis for security and performance.

Any unusual wireless network event that may reflect unauthorized use of wireless network services should be immediately reported through the OIT for review and, if appropriate, investigation. Such reportable events include the discovery of unauthorized Wireless Access Points on any MSU properties.

POLICY

Responsibility for Wireless Access Points: Campus responsibility for electronic communication resources reside with the Office of Information Technology, who must approve all installations of wireless access points used on all campus sites.

- Wireless equipment and users must follow PG-55 “Technology Resource Acceptable Use”. Wireless services are subject to the same rules and policies that govern other electronic communications services at the University.

- Abuse or interference with other activities is a violation of acceptable use. Interference or disruption of other authorized communications or unauthorized interception of other traffic is a violation of policy.
- Radio communication, due to its dependence on a scarce and shared resource, is subject to additional rules concerning interference and shared use.
    1. Wireless access points must meet all applicable rules of regulatory agencies, such as, the Federal Communications Commission and Public Utilities Commission.
    2. Wireless access points must be installed so as to minimize interference with other RF activities particularly as described below.
- Only hardware and software approved by the Office of Information Technology or designee shall be used for wireless access points.

Security: General access to the network infrastructure, including wireless infrastructure, is limited to individuals authorized to use campus and Internet resources.

- Physical security of wireless access points is maintained to protect the access point from theft or access to the data port.
- Access points shall enforce user authentication at the access point before granting access to secured campus or Internet services. Wireless network interfaces shall support authentication to access the secured campus wireless network.

Network Reliability and Interference

In a wireless environment, network reliability is a function both of the level of user congestion (traffic loads) and service availability (interference and coverage). In an effort to provide an acceptable level of reliability, this policy establishes a method for resolving conflicts that may arise from the use of the wireless spectrum.

Wireless networking technology uses unlicensed frequency bands to create small local area network cells. Since unrelated devices such as cordless telephones, wireless audio speakers, and even microwave ovens may also use these same frequency bands, the potential for disruption of service exists when multiple devices are placed in close proximity to one another.

While OIT does not actively monitor use of the frequency spectrum for potential interfering devices, it responds to reports of specific devices that are suspected of causing interference and disruption of the campus network. Where interference between the campus network and other devices cannot be resolved, OIT reserves the right to restrict the use of all wireless devices in University-owned buildings and all outdoor spaces.

Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited.

- In the event that a wireless device interferes with other equipment, the OIT or designee shall resolve the interference as determined by use priority.
- If other equipment interferes with a wireless device, the OIT or designee shall resolve the interference as determined by use priority.
- The order of priority for resolving unregulated frequency spectrum use conflicts shall be according to the following priority list: instruction, administration, research, and public access.
- Any unapproved or rogue access points found connected to the network will be disabled.
- New plans for buildings and gathering areas must consider the need for and use of wireless networking.